BAKER BOTTS L.L.P.
30 ROCKEFELLER PLAZA
NEW YORK, NEW YORK 10112

TO ALL WHOM IT MAY CONCERN:

Be it known that I, Jürgen Büssert, a citizen of Germany, residing in Igensdorf, whose post office address is Krumme Leithe 3, 91338 Igensdorf, Germany, have invented an improvement in:

ENCRYPTION OF CONTROL PROGRAMS

of which the following is a

SPECIFICATION

FIELD OF THE INVENTION

[0001] The present invention relates to a method and a system for transferring control programs, particularly in connection with the configuration, project engineering and commissioning of control systems which require the transfer of control programs.

BACKGROUND OF THE INVENTION

[0001] The control programs for programmable controllers are generally compiled in development or engineering systems. In addition to compiling control programs, engineering systems are also used for the commissioning, project engineering and configuration of controllers and drives.

[0002] It is quite usual for the compilation of the control programs to be carried out by a first specialist team and the commissioning, project engineering and configuration to be carried out by a second specialist team, with the two specialist teams being separated physically from each other. This means that the control program compiled by the first specialist team has to be transmitted to the second specialist team. It is often desirable to be able to use a quick transmission route but without loss of confidentiality during the transmission in order that to ensure that certain knowhow is not accessible to unauthorized third parties.

SUMMARY OF THE INVENTION

[0003] The object of the present invention is therefore to provide a method and a system which enables the transfer of control programs quickly but without losing confidentiality. This objective is achieved by a method of transferring control programs by encrypting a control program code in a first development system, transferring the encrypted control program code from the first development system to a second development system and decrypting the encrypted control program code in the second development system. The desired objective is further achieved by a system for transferring control programs having a first development device for developing a control program code. This device comprises an encryption unit for encrypting the control program code, a communications device for transferring the encrypted control program code from the first development device to a second development device. The second development device comprises a decryption device for decrypting the encrypted control program code. The present invention makes it possible to protect the knowhow on which

the control program is based without compromising the speed required to transfer the control program.

BRIEF DESCRIPTION OF THE DRAWING

[0004] The present invention is explained in greater detail below with reference to the drawing in which Figure 1 illustrates a data flow chart according to a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0005] The compiler and supplier of a control program develops the program in project engineering software or engineering system 1. The customer receives this control program via the Internet 2 or any other desired network or other connection. The customer integrates the control program received into his engineering system 3 and can therefore drive his target hardware (run-time system) 4.

[0006] In order that the control program is not accessible in all its details during the transmission in public networks to the customer, the control program is wholly or partially encrypted. This may be carried out by means of standardized encryption techniques, for example the PGP method using symmetrical or asymmetrical keys.

[0007] More specifically, the supplier first compiles an unencrypted control program 5 and stores it in a long-term data holder 6. The unencrypted program 5 or program code 7 can be loaded by the supplier 6 into a program editor 8 which is part of the engineering system 1. In the editor 8, the supplier can edit the program and, in order

to encrypt the program, can start up a postprocessor 9, which outputs an encrypted program code 10. For the purpose of encryption, the postprocessor 9 uses a key 11. The standardized PGP method is typically used for encryption. In the case of asymmetrical encryption, the supplier uses a "public key" for the encryption, and the customer uses the matching "private key" 12 for the decryption.

[0008] In order to transmit the encrypted program code 10, for example via the Internet 2, the data is initially exported from the project engineering software 1. Here, the data is preferably converted into HTML or XML format, or another format that can be read by standard Internet clients. The advantage of data formatted in this way resides in the fact that access to the data can be obtained with standard tools, and the user does not necessarily have to have an engineering system. After export, the encrypted XML data 13 is stored, for example, in a public web server 14 which makes the encrypted control program available only to a specific, desired client group, in the XML format for generality or in accordance with the encryption technique.

[0009] The customer loads the encrypted XML data 13 into his long-term data holder 15. From the data holder 15, the data is imported into the engineering system or the project engineering software 3 belonging to the customer. If the engineering system 3 of the customer is not based on the XML format or another format that can be read by standard Internet clients, conversion of the data into the engineering system format takes place during the import, the corresponding, encrypted program code 16 being generated. The customer is then able to edit the encrypted program code 16 in his program editor 17, which is again part of the engineering system 3.

[0010] Depending on the depth of encryption, the customer is in a position to edit only the data desired by the supplier. For example, it is possible to encrypt the data to any desired depth in the horizontal and vertical direction. Encryption on a specific horizontal plane means that, for example, modules at the same functional level are encrypted differently. For example, a library having the functions a, b, c and d may be encrypted with a number of pairs of keys so that the customers A, B, C and D can decrypt and use only the modules intended for them in each case. Vertical encryption means different encryption at different hierarchical, functional levels. For example, it is conceivable that a customer merely has to know the module parameters, including the return parameters, in order to operate the control program. The head of the control program can therefore remain unencrypted, while the core of the program is encrypted. This is used in particular for the purpose of protecting the knowhow on which the software is based. Furthermore, the software program can also be completely encrypted for the purpose of transmission and processing by the customer and, for example, only capable of being decrypted completely by the service personnel. Further, arbitrary granular types of encryption are also conceivable which correspond to the modular construction of a control program.

[0011] Following editing, the wholly or partly encrypted control program is decrypted in a preprocessor 18 belonging to the engineering system 3. For this purpose, the preprocessor 18 uses the private key 12. The decrypted program code 19 obtained from the preprocessor 18 is converted in a compiler 20 into microprocessor-specific, executable binary code 21, which is then loaded by the project engineering software or

the engineering system 3 into the target hardware or a run-time system 4. There, the binary code is processed by a microprocessor.

[0012] The aforementioned integration of an encryption system into engineering systems, using asymmetrical keys 11, 12, results in the following advantages:

- The known routines for encryption and decryption convert from ASCII text into ASCII text. The encrypted areas may therefore be saved and transported in the same way as the unencrypted areas, and therefore provide ideal integration into the widespread XML format. In particular, standard tools may be used for the further processing of the data.

- Because of the use of a text format, it is also possible for parts of a text to be encrypted. Therefore, as already mentioned, the head of a program with Defines, as they are known, for adaptation can remain unencrypted, while the body of the program having the functions is protected.

- The supplier of user software, for example compiler or project engineering tool, provides its own pair of keys. In the case of asymmetrical encryption, the supplier keeps the public key with the customer data of the user. Therefore, the supplier can, for example, encrypt libraries for specific customers by using their public key and transmit them to these customers via any desired channel. Accordingly, copying the user software provided via public channels is senseless since the library can be

decrypted only for the application of the envisaged customer. Hence, a license system can easily be implemented.

- The encrypted texts cannot be analyzed. The internal knowhow therefore remains protected.

- As a result of the integration of asymmetrical decryption into a preprocessor belonging to the compiler, parts of the program can be protected against misuse without changing the compiler itself. The preprocessor runs only during the generation of the binary code for the target system. Furthermore, the program editor also does not require any change, since the encrypted texts are displayed as such.

[0013] The system according to the present invention described above may be modified with the effect that the encryption is incorporated directly into the export mechanism and the decryption is incorporated directly into the import mechanism. However, all the data from the control program will be released to the customer for editing.